Kiteworks

COMPLIANCE BRIEF

Navigating New SEC Cybersecurity Disclosure Rules

Kiteworks Supports Timely, Accurate Reporting

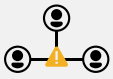
Public companies just got handed sweeping new cybersecurity reporting rules by the Securities and Exchange Commission (SEC) that will force them to open their books on data breaches and cyber risks. Under Form 8-K Item 1.05, companies now must report material cybersecurity incidents within a mere four days of occurrence. Form 6-K will be amended to require foreign private issuers to disclose information on material cybersecurity incidents in a foreign jurisdiction to any stock exchange or to security holders. Additionally, under Regulation S-K Item 106, companies need to disclose their cybersecurity risk management processes in detail to investors, and add to annual filings in 2023 their entire cyber risk management strategy and past incidents. The goal is to provide more transparency for investors on cybersecurity programs, risks, and impacts. All public companies must comply with the annual disclosures starting with reports for fiscal years ending after December 15, 2023. For material breach reporting, most companies must comply beginning 90 days after the rules' publication in the Federal Register or by December 18, 2023. Smaller reporting companies have until June 15, 2024, to begin 8-K disclosures. The SEC goal is clear visibility for investors on cyber threats, governance, and impacts. Kiteworks' audit logging and security alert capabilities empower agencies to monitor cyber risks proactively, detect incidents faster, and have the forensic evidence required for detailed SEC reporting within tight time frames. Here's how:

Increased Reporting Regulation

The SEC's Regulation S-K Item 106(b) requires public companies to disclose their processes for assessing, identifying, and managing material cybersecurity risks in their regular SEC filings. Companies must describe how these processes are integrated into their overall risk management system and whether third parties are engaged to support cyber risk management. They must also discuss whether any prior incidents have materially impacted the business and how cyber risks may affect strategy and performance going forward. The SEC also now mandates that public companies disclose material cybersecurity incidents within four days under Form 8-K Item 1.05. This includes detailing the nature, scope, timing, and business impacts of the breach. Finally, the SEC's Form 6-K requires public companies to promptly disclose any cybersecurity risks or incidents that are material to investors. To comply, organizations need capabilities to detect threats early and have detailed forensic evidence to investigate incidents.

Solution Highlights

Comprehensive audit logs



Security alerts

Integration with SIEM solutions

Centralized visibility

Real-time monitoring

Comprehensive Governance Oversight

Regulation S-K Item 106(c) requires companies to describe the board of directors' oversight of risks from cybersecurity threats and management's role and expertise in assessing and managing these risks. This disclosure is mandatory in annual reports on Form 10-K and Form 20-F. It includes identifying any board committee or subcommittee responsible for the oversight of cybersecurity risks and describing the processes by which the board or such committee is informed about such risks. The board oversees cybersecurity risks, including risks from external file sharing, through the Audit Committee. Kiteworks supports regular updates on cyber risks and mitigation plans, including details on Kiteworks' role-based access policies that control external collaboration. Kiteworks allows granular control over file sharing permissions to limit access to sensitive data. Features like restricted email forwarding, user access reviews, and content scanning protect intellectual property and private information while enabling secure collaboration. Centralized policy administration and transaction inspection ensure consistent enforcement enterprise-wide. Detailed audit logs provided by Kiteworks give managers and auditors the reports needed to prove regulatory compliance. With its robust access controls and auditing, Kiteworks aids governance of cyber risks stemming from external digital content exchange.

Organizations must describe management's role in assessing and managing the registrant's material risks from cybersecurity threats. Kiteworks allows management to utilize controls, monitoring, and threat prevention to mitigate cyber risks from third-party partnerships. Granular access policies ensure external collaborators only access data necessary for their role. Real-time monitoring tracks all user activity, file transfers, and data access, while encryption and hashing technologies secure information and ensure its integrity. Together, these capabilities prevent unauthorized data access and modification, reducing the attack surface. Additionally, integration with SSO, MFA, AV, ATP, and DLP solutions provides layered security aligned to industry best practices. Audit logs demonstrate compliance during regular reviews and audits. By restricting access, detecting threats, and protecting sensitive assets, Kiteworks enables safe external collaboration while empowering management to maintain strong data security governance. The platform's defense-in-depth approach is a key part of the company's program to assess and mitigate third-party cyber risks.

Disclosures must also be made surrounding whether and which management positions or committees are responsible for assessing and managing such risks, and the relevant expertise of such persons or members in such detail as necessary to fully describe the nature of the expertise. Kiteworks helps companies comply with SEC Regulation S-K Item 106(c)(i) by providing robust access controls and auditing to secure external collaboration. Granular role-based controls aligned to business need enforce least-privilege access, with custom folder permissions and viewer/uploader/editor roles limiting exposure. Locking mechanisms guarantee secure collaboration, while comprehensive monitoring provides visibility into all user actions. Detailed audit logs capture every transaction, allowing regular review to ensure policies are followed. By combining identity-centric access foundations with rich visibility, Kiteworks empowers proactive governance of external partnerships. Expert staff can analyze usage patterns to optimize permissions and detect suspicious anomalies. Both preventative access limitations and detective controls aid risk reduction and regulatory compliance. Kiteworks is a critical component of a cyber-secure framework for collaborating securely with external parties.

Additionally, organizations need to disclose the processes by which these people or committees are informed about and monitor the prevention, detection, mitigation, and remediation of cybersecurity incidents, and whether they report information about the risks to the board of directors or a committee or subcommittee of the board of directors. Kiteworks aids governance and reporting on cyber risks as required by SEC Regulation S-K Item 106(c)(ii) and (iii). Leveraging Kiteworks' dashboards, audit logs, and alerts empowers oversight and reporting of cyber incidents. The CISO and Governance Committee monitor the platform's security analytics for suspicious anomalies that may necessitate investigation and remediation. Comprehensive activity logging captures every user transaction, allowing regular audits to ensure policies are followed and detect potential insider threats. In case of a confirmed breach, instant notifications activate established response protocols to mitigate impact. Risks are reported up to the board either directly by the CISO or via the Audit Committee, which has cybersecurity as a standing agenda item. Kiteworks provides continuous visibility, enabling expert staff to monitor prevention efforts, swiftly detect intrusions, and keep leadership apprised of cyber health. Detailed alerts and records support SEC requirements for informing and involving executives and directors in cyber risk governance through vigilant monitoring and timely reporting.

Audit Logs and Security Alerts Provide Visibility and Support Compliance

To meet these stringent regulations, Kiteworks provides critical capabilities for security monitoring, incident detection, and detailed forensic auditing. Kiteworks delivers comprehensive, immutable audit logs capturing all user, admin, and file activity across its secure platform. These centralized logs support routine oversight of cyber risks and rapid forensic analysis when an incident occurs. Audit logs establish a chain of custody to determine what data was accessed, when, and by whom to quantify breach impacts. Logs easily integrate with SIEM solutions for automated alerting, reporting, and response workflows. Furthermore, Kiteworks' configurable alerts notify administrators of suspicious events like failed logins or abnormal file transfers that may indicate threats. Together, Kiteworks' robust activity logging and automated alerts deliver the cyber risk visibility and early threat detection organizations need to comply with SEC disclosure rules. The audit logs rapidly facilitate investigating, remediating, and reporting material cyber incidents within four days as required. The alerts enable proactive monitoring to identify issues faster and minimize impacts. With comprehensive activity tracking and alerts across collaboration tools, Kiteworks strengthens cybersecurity oversight, incident response, and forensic capabilities essential for detailed SEC reporting. It empowers enterprises to meet new transparency regulations, safeguard sensitive data, and uphold investor trust. Ultimately, Kiteworks provides the security visibility, controls, and actionable threat insights organizations need to demonstrate effective cyber risk governance, resilience, and timely disclosure.

The SEC now requires detailed disclosures on cyber risks and material data breaches. Kiteworks provides the capabilities crucial for meeting these regulations, including comprehensive audit logs capturing detailed activity trails and configurable alerts to detect threats early. Kiteworks' robust logging enables rapid forensic analysis to investigate and disclose incidents within the SEC's tight four-day window. Its alerts facilitate proactive monitoring to identify issues faster and reduce impact. By securing access to sensitive content, detecting anomalies, and providing audit logs, Kiteworks helps companies prevent, detect, and respond to potential cybersecurity incidents. Its security capabilities empower enterprises to comply with the SEC's stringent disclosure requirements, uphold investor trust, and demonstrate effective cyber risk governance. For public companies, Kiteworks is critical for timely, accurate reporting on cyber incidents now strictly mandated by the SEC.